

Legal Commentary

November 16, 2021

Timely Move: MIIT to Strengthen Data Security Management in the Field of Industry and Informatization

Authors: Kevin DUAN | Kemeng CAI | Tina WANG

On September 30, 2021, The Ministry of Industry and Information Technology (“**MIIT**”) issued for public comments the *Measures for Administration of Data Security in the Field of Industry and Informatization (for Trial Implementation) (Draft for Comment)* (the “**Measures**”). The Measures are the first regulatory document (draft for comment) in the field of data security to be formulated by industry regulators following the effectiveness of the Data Security Law and would create a series of new tasks and requirements for enterprise data compliance.

The core contents of the Measures are summarized as follows:

- **Scope of application.** The Measures regulate all industrial and telecom data processing activities carried out within China. Regulated subjects include all types of enterprises in the software and information technology service industry as well as enterprises that hold telecoms business licenses, as well as apps operators in “software and information technology service industries” that provide products and services through apps. The Measures apply to all personal information processing activities.
- **Scope of important data and core data and enhanced administrative requirements.** The Measures refine the principles for identifying important data and core data from perspective of the degree of potential harm resulting from data leaks while they do not provide examples of data types that are considered important data or core data. The aforesaid principle will provide support for the assessment of effects of important data or core data on the national security risk stipulated under the Measures for Cybersecurity Review (Revision Draft for Comment). In addition, the Measures also strengthen management requirements for core data and important data from various aspects, including working systems, data storage, data transmission, and data cross-border transfer. Notably, the Measures for the first time call for a prohibition on the export of core data.

- **Filing and reporting obligations.** The Measures stipulate filing and reporting obligations for data processors on the processing of important data and core data. Those obligations, as well as strengthened management requirements for important data and core data (including data export requirements), demonstrate the regulator's attitude and approach in urging data processors to implement relevant supervision requirements.
- **Enterprises must clearly designate a data security responsible person and undertakes full lifecycle data security protection obligations.** Enterprises are required to specify the person and department responsible for data security management and, where processing of important data or core data are involved, designate a department to be specially responsible for data security management and allow the Party committee (Party group) or leading body be in charge of data security. Furthermore, enterprises should ensure the full lifecycle of data security compliance in accordance with the Measures.
- **Conduct security assessments and cooperate in data security reviews.** Enterprises should implement data security assessments and make data rectification according to data grades. Specifically, enterprises should conduct self-assessments for general data and conduct annual security assessments and fulfill reporting obligations for important data and core data. Where processing of important data or core data affects or may affect national security, such data processing activities may be subject to data security review and, in some cases, may be subject to a cybersecurity review.

Below, we summarize and comment on the key requirements regarding data security management for industrial and telecoms industries data under the Measures.

Extensive application scope: multi-dimensional supervision of personal information and exceptions in specific industries

The Measures provide an extensive application scope, specifying data types and enterprise types subject to regulation. Specifically, industries subject to the Measures may include Internet, Internet of Vehicles, autopilot, artificial intelligence, and cloud computing. Furthermore, enterprises in sectors such as healthcare, finance, and hospitality that hold telecoms operating licenses may also be subject to the Measures. In addition, the Measures could also apply to all app operators, regardless of industry, if the term “software and information technology service industries” is interpreted as products and services provided through apps.

The Measures at Article 2 specifically defines their scope of application—the Measures apply to data processing and security monitoring of industrial and telecoms data carried out within mainland China. According to Article 3, “**telecoms data**” refers to data collected and generated in the course of telecoms business operations; “**industrial data**” refers to data collected and generated in the business process of “R&D and design, manufacturing, operation and management, operation and maintenance services, platform operations, and application services” in the fields of “raw material industries, equipment industries, consumer goods industries, electronic information and manufacturing industries, software and information technology service industries, and industrial explosive materials industries”; “**industrial and telecom data**

processors” refer to all industrial enterprises, software and information technology service providers, and telecoms business operators with telecoms operating licenses as well as other entities engaged in data processing of industrial data and telecoms data.

It is worth noting that the Measures have no extraterritorial effect, unlike the Data Security Law and the Personal Information Protection Law. In addition, the Measures in Chapter VIII exclude the application of the rules for data processing activities that involve state secrets, password use, military data, government data, data in science and technology industries, and the tobacco industry.

The Measures also stipulate extensive data types subject to their scope. Adhering to the philosophy of the Data Security Law, which emphasizes control over personal information by categorizing it in the catalogue of important data and core data, the Measures also adopt strengthened supervision of personal data by implementing lifecycle security management of personal information¹. Thus, enterprises must fulfil their personal information protection obligations by complying with relevant laws and regulations on protection of personal information and also by conforming to the data security management requirements under the Measures.

The MIIT and cyberspace administration departments have long been engaged in regulatory and enforcement activities with respect to personal information processing by apps. Enterprises handling personal information are thus subject to supervision by multiple departments. The Measures cite as their enabling laws the Cybersecurity Law and the Data Security Law, not the Personal Information Protection Law. This signals that MIIT will focus to an extent on the regulation of data in the industrial and telecoms fields, while it will not include all types of personal information in its purview.

Important data and core data: specifying industries and potential level of harm resulting from data leaks

The Measures reiterate the method of data classification and data grading stipulated under the Data Security Law, requiring that enterprises adhere to the principle of “first classify data, then grade data”. Specifically, industrial and telecoms data is to be categorized into **research and development data, production and operations data, management data, operation and maintenance data, business service data, and personal information** (Article 7); in terms of data grading, industrial and telecoms data will be divided into three grades according to the criteria set forth in Articles 8 to 10: **general data, important data, and core data**.

Data whose leakage will cause the following consequences will be defined as **important data**:

- Threatening to political, territorial, military, economic, cultural, social, scientific and technological, cyber, ecology, resource, and nuclear security, possibly affecting data security in key state areas such as overseas interests, biology, space, polar regions, deep sea, and artificial intelligence;

¹ See *Administrative Measures on Data Security in the Field of Industry and Informatization (for Trial) (Draft for Comment)* by clicking: https://www.miit.gov.cn/cms_files/filemanager/1226211233/attach/20219/1d1668e46e644b42b04a95db43854607.pdf.

- Interfering with the development, production, operation, and economic interests of industrial or telecoms industries;
- Causing major data security incidents or work safety accidents, which have a serious impact on public interests or legitimate rights and interests of individuals or organizations, and have substantial negative social impacts;
- Causing obvious cascading effects, having widespread influence that spread to multiple industries, regions, or multiple enterprises within the same industry, or having long-term effects that significantly prevents industrial development, technological progress, and industrial ecosystems; or
- Paying high prices for recovery of the data or elimination of negative impacts.

Data whose leakage will cause the following consequences will constitute **core data**:

- Severely threatening the political, territorial, military, economic, cultural, social, scientific and technological, network, ecosystems, resources, and nuclear security, and seriously affecting data security in key state areas such as overseas interests, biology, space, polar regions, deep sea, and artificial intelligence;
- Severely affecting industrials and telecoms and their important “backbone” enterprises, critical information infrastructure, and important resources; or
- Severely damaging the industrial production and operation, telecoms, Internet operations and services, resulting in wide-ranging business shutdowns, wide-ranging network and service breakdowns, and massive loss of business processing capabilities.

From the above definition, we understand industrial and telecoms data that may have an impact on national security may be regarded as important data, even core data. That also constitutes the basis for the national security-oriented *Measures for Cybersecurity Reviews* (Revision Draft for Comment), which includes in its scope of review “risk of theft, leakage, damage, illegal use or export of core data, important data or large amounts of personal information”.

However, enterprises still await clearer guidance in practice on specific standards for the grading of the industrial and telecoms data, because the Measures merely stipulate general principles for assessing the consequences of leakage of relevant data and lack specific standards to identify how the leak would “severely threaten”, “severely affect”, or “severely damage” relevant industries. In addition, as the local departments of industry and information technology and communication administrations would be responsible for formulation and reporting of the catalogues of important data and core data for specific industries and regions, the scope of important data and core data remains to be further specified by the MIIT following the implementation of the Measures.

Reporting and filing: increase transparency of data processing

According to Article 11 of the Measures, the government will establish a “MIIT – local authorities – data processor” three-level linkage data classification and grading system in the field of industry and information

technology, and will accordingly establish a series of working mechanisms in the future, such as data classification and protection mechanisms, a mechanism for reporting and filing of important data and core data, etc. Under this data management system, enterprises mainly have the following three types of compliance obligations:

- **First, the enterprises must classify data into different catalogues and develop data lists, and thereby determine lists of important data and core data.** Enterprises must review the data classification and grading on regular basis and update the list from time to time.
- **Second, enterprises must implement hierarchical protection of the classified and graded data.** Enterprises must exercise special protection for important data, and implement stricter management and protection of core data. Where data of various grades are processed at the same time and it is difficult to separately adopt protective measures for each specific grade of data, protective measures applicable to the highest grade are to be adopted.
- **Third, enterprises are responsible for reporting and filing of important data and core data after the data classification and grading.** Enterprises are required to report important data and core data catalogues to the local industry and information technology authorities or communications authorities, and file important data and core data according to relevant requirements. If there is any change in the filed data², the enterprises should report such change to the filing authority within three months, and update the filed contents.

For data included in the reporting catalogue of important data and core data, enterprises should exercise enhanced protection on such data according to the requirements in the Measures in full lifecycle of data processing.

Leadership responsibility for data security: detailed description of responsibilities and leaders' responsibility

The first step for enterprises to fulfill their data security management obligations is to establish and improve their data security leadership system according to the Measures. The Measures set detailed requirements for departments and personnel responsible for data security management, requiring enterprises to specify the department and person in charge of data security management, and specify key positions and personnel involved in data processing.

For enterprises involved in processing important data and core data, the Measures further provide that the Party committee (group) or leadership team will undertake primary responsibility for data security; the head of the enterprise is the first responsible person for data security; and the person in charge of data security is the person directly responsible for data security. Furthermore, the enterprises should designate a department especially responsible for data security. Therefore, we recommend enterprises that process important data and core data to examine and adjust their organizational structures going forward, and to adjust their current organizational structures where various data security responsibilities fall onto one sole

² The filed contents include basic information of data such as the quantity, type, purpose of processing and method of processing, scope of usage, responsible party, and security measures, as well as information on data provision, disclosure, cross-border transfer, undertaking, data security risks, incident handling, etc. See Article 12 of the Measures.

department or officer, so as to meet requirements of the Measures to implement enhanced protection of important data and core data.

Life-cycle security management: a manifestation of national security and public interests

Compared with the Data Security Law and the Cybersecurity Law, which only provide general provisions on data protection, the Measures, following concepts of the *Measures for Administration of Data Security (Draft for Comment)*, which not only set out the general requirements for protection of various grades of data in full life-cycle of data management, but also stipulate additional requirements on the processing of important data and core data. The Measures set forth specific compliance requirements for enterprises, stipulating detailed requirements on execution of data security agreements and commitment letters, and maintenance of processing records, which will provide guidance for enterprises to fulfill their data security management obligations. In order to fulfill the full life-cycle of data security obligations, we recommend enterprises to pay special attention to the following compliance requirements:

- Without the consent of relevant individuals or entities, enterprises may not create accurate portraits, conduct data restoration, or carry out other data processing activities with respect to any specific person.
- Enterprises must destroy industrial and telecoms data they maintain upon receipt of third-party accredited request, if such request is raised for the purpose of protecting national security and social and public interests.
- Enterprises must establish registration and approval mechanisms for the transmission of general data, the supply of important data, and the use and processing of important data and core data, which impose higher requirements on enterprises for the establishment of internal procedures and maintenance of data processing records.
- Enterprises must obtain state approval for the transmission and supply of core data.
- Important data must be stored within mainland China. If enterprises truly need to transfer important data cross-border, they should conduct a data export security assessment according to laws and regulations. Under no circumstances may core data be transmitted abroad.

Pursuant to the Data Security Law³ and the Cybersecurity Law⁴, the cyberspace administration and

³ Article 31 of the Data Security Law stipulates that: “The security administration of the cross-border transfer of important data collected and generated by operators of critical information infrastructure during their operation in China shall be subject to the provisions of the Cybersecurity Law of the People’s Republic of China; the administrative measures for the cross-border transfer of important data collected and generated by other data handlers during their operation in the People’s Republic of China shall be formulated by the national cyberspace administration authority in collaboration with relevant departments of the State Council.”

⁴ Article 37 of the Cybersecurity Law stipulates that: “Critical information infrastructure operators shall store personal information and important data gathered and produced during operations within the territory of the People’s Republic of China. Where it is truly necessary to provide such information and data to overseas parties due to business requirements, a security assessment shall be conducted in accordance with the measures formulated by the national cyberspace administration authority in concert with the relevant departments under the State Council. Where the laws and administration regulations have other provisions, those provisions shall prevail.”

relevant departments of the State Council are responsible for the formulation of the rules on cross-border transfers of important data. As the Measures do not stipulate specific requirements for the export of general data, storage and export of general data will be subject to certain restrictions if such data are subject to special regulations. For example, the export of personal information is governed by provisions of the Personal Information Protection Law.

Security assessment, monitoring and inspection, data security review: uncertainty under the institutional framework

According to Chapters V and VI of the Measures, the State will implement data security supervision and administration through data security inspection, assessment, authentication, supervision, inspection and security review.

I Conducting security assessments

According to Article 33 of the Measures, enterprises may conduct data security self-assessments for general data, and should conduct annually security assessments of important data and core data and **report** their important data and core data catalogues to the local authorities. Notably, Article 33 of the Measures permits enterprises to conduct self-assessments either on their own or to entrust a third party to do so.

II Assisting with supervision and inspection

According to Article 34 of the Measures, enterprises are obligated to cooperate with industry regulators in their supervision and inspections and reserve a specific inspection interface. However, the Measures do not clearly provide for issues of concern to enterprises such as the scope of inspection, technical standards of the inspection interface, and interface access conditions. Clear guidance in practice is still necessary from the competent authorities as to requirements on setting of inspection interfaces.

III Passing data security review

Similar to Article 24⁵ of the Data Security Law, the Measures provide at Article 35 that the MIIT will, under the coordinated working mechanism for national data security review, conduct data security reviews of processing of industrial and telecoms data that affect or may affect national security. However, the Measures do not specify under which conditions the review process will be launched or the specific process of the review work. In addition, the *Measures for Cybersecurity Review (Revision Draft for Comment)*, which were released on July 10, 2021, subject data processing activities into the scope of review, stipulating that data processing risk factors for assessment include “risk for core data, important data or massive personal information to be stolen, leaked or destroyed, or illegally used or taken abroad”. Therefore, enterprises that process industrial and telecoms data may have to go through dual reviews under the Measures and the Measures for Cybersecurity Review.

⁵ Article 24 of the Data Security Law stipulates that: “The State shall establish a data security review system, where data handling activities that affect or may affect the national security will undergo national security review.”

Conclusion

MIIT plays an irreplaceable and important role in the data security regulatory system, as it administers multiple industries that are fundamental and critical industries to the development of the digital economy, including equipment and consumer goods industry, the telecoms industry, the electronic information manufacturing industry, the software industry, and the Internet industry. The industry and telecoms administrations rank first among industry administrations in the Data Security Law for undertaking data security supervision responsibility for specific industries. This indicates that industrials and telecoms are important industries for strengthening data security management. The Measures clarify the criteria for identifying important data and core data in the industrial and telecoms industries, and provide strengthened and practical compliance requirements for important data and core data security protection, to which enterprises in the industrial and telecoms industries should pay great attention.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Kevin DUAN

Tel: +86 10 8516 4123

Email: kevin.duan@hankunlaw.com